Information Security Oversight Office
Washington, DC 20405

DRAFT

December 21, 1987

Dear Mr. Chairman:

The Information Security Oversight Office (ISOO) encloses answers to the questions posed in your letter of November 13, 1987, regarding the Standard Form 189, "Classified Information Nondisclosure Agreement."

Sincerely,

Steven Garfinkel
Director

The Honorable
Gerry Sikorski
Chairman
Subcommittee on Human Resources
Committee on Post Office and Civil Service
House of Representatives
Washington, DC 20515

Enclosure

DRAFT

December 21, 1987

I. BASIS AND NEED FOR NONDISCLOSURE AGREEMENTS

1. Please explain what national security concerns addressed by SF 189 would remain unsolved if employees holding security clearances instead were required to sign the following agreement: "I am aware of my duty to protect classified information, have been trained in my responsibilities to protect classified information and pledge to honor my duty to protect classified information."

ANSWER: The SF 189 is not a unilateral promise, such as the oath suggested in the question, but a contract supported by consideration on both sides. The form is a standardized nondisclosure agreement which alerts employees of the trust that is placed in them by providing them access to classified information and of their responsibilities to protect that information from unauthorized disclosure. It also states the nature of that trust and those responsibilities, so that if that trust is violated, the United States will be in a better position to enforce the agreement. By specifying the rights and duties of the parties in the form of a contractual agreement, SF 189 is far more informative and educational than the oath suggested in the question. Both the employee and the agency are better informed of their specific rights and duties. Among the specific references contained in it, SF 189 cites the laws that may apply if an employee makes an unauthorized disclosure of classified information, and also notes what legal remedies may be available to the United States. Further, SF 189 stipulates the time period that its provisions apply, and the means by which an employee may be relieved of the obligation to protect information that was classified at the time of the employee's access to it.

I. 2. What specific statutes have failed to adequately protect classified information? Please reference any unsuccessful attempted prosecutions, or the facts of any case that the Department of Justice wanted to prosecute in this area but declined due to weaknesses in existing statutes.

ANSWER: There is no specific statute, per se, that "has failed to adequately protect classified information." There have been some persons within the executive branch during this and prior administrations who have argued in support of additional criminal statutes to sanction those who disclose classified information without authority.

Beyond the issue of criminal statutes, however, the Administration has never taken the position that criminal sanctions alone are the only appropriate means to respond to unauthorized disclosures. Civil and administrative sanctions are also necessary tools to help prevent and punish the unauthorized disclosure of classified information.

I. 3. What legislative proposals has the administration made to plug these statutory loopholes? Please be specific in matching particular provisions of any proposed legislation to the individual loopholes that have frustrated prosecutions or other personnel actions.

ANSWER: None.

I. 4. In the absence of SF 189 why can't any agency take an adverse action on the grounds of impeding the efficiency of the service, against an employee who improperly discloses sensitive information?

ANSWER: We assume that your reference to sensitive information refers to classified information. In the absence of

a nondisclosure agreement an agency may take an adverse action on the grounds that an unauthorized disclosure impedes the efficiency of the service in accordance with Civil Service laws and agency regulations, providing the facts and circumstances merit such action. The SF 189, however, alerts employees of the trust that is placed in them by providing them access to classified information and of their responsibilities to protect that information from unauthorized disclosure. It also states the nature of that trust and those responsibilities, so that if that trust is violated, the United States will be in a better position to enforce the agreement in the context of its contractual provisions. Finally, SF 189 provides for other remedies in addition to the remedy of adverse action.

I. 5. What and how many national security leaks have occurred due to the release of information that is classifiable but not classified? Please specify the definition of classifiable upon which you base this answer.

ANSWER: "Classifiable information," as used in SF 189, generally refers to unmarked classified information. In these situations, therefore, there cannot be an unauthorized disclosure of "classifiable information" that is not also an unauthorized disclosure of classified information. The only "classifiable information" that is not yet classified refers to information that is in the process of a formal classification determination. In these situations we are aware of no unauthorized disclosures.

I. 6. Who in the National Security Council (NSC) authored SF 189? Who in the NSC reviewed and approved the nondisclosure agreement? Who in the Department of Justice reviewed the form before and since its release?

ANSWER: The NSC staff was not the author of SF 189. The form is a product of an interagency working group formed to fulfill the requirement contained in National Security Decision Directive 84 to develop a legally enforceable standardized nondisclosure agreement. Chaired by the Director of ISOO, the interagency working group included representatives designated by the Secretaries of State, Treasury, Defense and Energy, the Attorney General and the Director of Central Intelligence. National Security Advisor William P. Clark approved SF 189 for the President on August 10, 1983. The form has been reviewed by attorneys and other officials in the Department of Justice, including the Office of the Attorney General, the Office of Legal Counsel, the Civil Division, the Criminal Division, and the Office of Security. Richard K. Willard, Assistant Attorney General, Civil Division, provided ISOO with formal notification of the validity and enforceability of SF 189.

I. 7. What public interest groups participated in the discussions preceding the issuance of SF 189? Did these groups review a summary of principles for a valid nondisclosure agreement or the specific language of SF 189?

ANSWER: ISOO's policy and practice have always been to maintain an ongoing dialogue on security classification issues with individuals and groups that are interested in this subject,

whatever their particular perspective on the issues. Representatives of the American Civil Liberties Union, its adjunct, the Center for National Security Studies, the National Classification Management Society, and the Association of Former Intelligence Officers discussed the issues surrounding nondisclosure agreements with ISOO. These discussions first dealt with principles and later, before any forms were executed, included the opportunity to review the specific language of the forms. In addition, congressional inquiries, including hearings, into National Security Decision Directive 84 commenced before SF 189 was put into effect, giving any number of other groups and individuals the opportunity to participate in the debate over nondisclosure agreements.

I. 8. What are the other, stronger nondisclosure agreements that have been upheld by the courts? Please provide legal citations for any such precedents.

ANSWER: The secrecy agreements used by the CIA have repeatedly been upheld by the courts. See United States v. Marchetti, 466 F.2d 1309 (4th Cir.), cert. denied, 409 U.S. 1063 (1972); United States v. Snepp, 595 F.2d 926 (4th Cir. 1979) (upholding secrecy agreement but denying government a constructive trust on Snepp's profits), rev'd, 444 U.S. 507 (1980) (affirming government's right to constructive trust); McGehee v. Casey, 718 F.2d 1137 (D.C. Cir.), reh'g denied, No. 81-2233 (D.C. Cir. 1983).

II. IMPLEMENTATION OF SF 189

1. Please list all agencies with employees who are required to sign SF 189.

ANSWER: Currently, the following executive branch departments, agencies, and offices are required to have their employees execute SF 189 as a condition of access to classified information:

Agency for International Development
Agriculture, Department of
Air Force, Department of the
Arms Control and Disarmament Agency
Army, Department of the
Board for International Broadcasting
Commerce, Department of
Council of Economic Advisers
Defense Advanced Research Projects Agency
Defense Communications Agency
Defense Contract Audit Agency
Defense Intelligence Agencyy
Defense Investigative Service
Defense Logistics Agency
Defense Mapping Agency
Defense Nuclear Agency
Defense, Office of the Secretary of
Education, Department of
Energy, Department of
Environmental Protection Agency
Export-Import Bank
Farm Credit Administration
Federal Communications Commission
Federal Emergency Management Agency
Federal Home Loan Bank Board
Federal Maritime Commission
General Services Administration
Health and Human Services, Department of
Housing and Urban Development, Department of
Interior, Department of the
International Trade Commission
Interstate Commerce Commission
Justice, Department of
Joint Chiefs of Staff, Organization of the
Labor, Department of
Management and Budget, Office of
Marine Mammal Commission
National Aeronautics and Space Administration

National Archives and Records Administration
National Science Foundation
National Security Council
Navy, Department of the
Nuclear Regulatory Commission
Office of Administration, Executive Office of the President
Overseas Private Investment Corporation
Peace Corps
Personnel Management, Office of
President's Foreign Intelligence Advisory Board
President's Intelligence Oversight Board
Science and Technology Policy, Office of
Securities and Exchange Commission
Selective Service System
Small Business Administration
State, Department of
Strategic Defense Initiative Organization
Tennessee Valley Authority
Transportation, Department of
Treasury, Department of the
United States Information Agency
United States Postal Service
United States Trade Representative, Office of the
Veterans Administration
Vice President, Office of the

The Central Intelligence Agency, Federal Reserve System and the National Security Agency received a waiver from NSC to use a substitute nondisclosure agreement that fully complies with NSDD 84.

II. 2. How many employees without security clearances have signed SF 189? What was the legal authority to require signatures by employees without security clearances? Is this practice still continuing?

ANSWER: ISOO does not know the actual count of employees without security clearances who have signed SF 189. There was no legal authority to require employees without security clearances

to sign SF 189. As ISOO has become aware of agencies that have done so, it has taken those steps necessary to stop this practice and to nullify the pertinent agreements.

II. 3. Were Oliver North, Fawn Hall, or William Casey at any time required to sign a nondisclosure agreement? If not, why not? If so, what agreement, and what enforcement actions have been taken, or investigations open, to hold Messrs. Casey and North and Ms. Hall, accountable for their potential violations of the nondisclosure agreement they signed?

ANSWER: Former Director Casey signed the CIA's secrecy agreement and the Sensitive Compartmented Information Nondisclosure Agreement, Form 4193. Both Fawn Hall and Oliver North signed SF 189 and Form 4193. ISOO is not aware of any investigation concerning alleged violations of these agreements.

II. 4. Do the explanations for SF 189 in the question and answer training pamphlet, DOD 5200.1-PH-1, have the force of law? In other words, is it a valid legal defense for an employee charged with SF 189 violations to prove that she/he relied on guidance from that training pamphlet? If not, why not? If not, please list all other non-binding explanatory materials that have been released, and upon which employees are not entitled to assert reliance to interpret the contract.

ANSWER: DOD 5200.1-PH-1 is not a legally binding supplement to the agreement embodied in SF 189. It is, however, an accurate guide to the intent of the Government in issuing and enforcing this agreement. The ISOO has read the guidance provided in the pamphlet and finds that it provides valid interpretations of some of the terms found in SF 189 and reasonable explanations of their intent. It, as well as all other explanatory materials formally

issued by agencies to explain SF 189, may be relied upon by employees as evidence of the proper interpretation of the nondisclosure agreement.

II. 5. Recently, through the Federal Register and correspondence with Congress, ISOO has issued a series of clarifying rules, notices and modifications to SF 189. To the extent that these or other new rules and/or notices modify the meaning of SF 189, can they ever be rescinded or further revised? If so, what procedure is necessary for modifications to be legally binding on a permanent basis? Please describe the boundary for what changes are permissible to SF 189s that already have been signed.

ANSWER: The regulatory clarifications to SF 189 that ISOO published in the Federal Register on August 3 and 11, 1987, are fully consistent with previous interpretations provided in response to individual inquiries and bind the Government on the interpretation of those provisions in existing versions and future reprints of SF 189. These regulatory changes do not in any way alter the substance of the agreement reflected in SF 189. To be legally binding, no modification to SF 189 can increase the legal obligations of the signer without his or her signature on that revised agreement.

II. 6. What retraining has the Administration initiated to correspond with all the recent clarifications? Has the retraining been consistently implemented for all agencies and employees covered by SF 189?

ANSWER: As clarifications have occurred, ISOO has alerted in writing each department, agency and office listed in the answer to question II. 1., above, about them. Because these clarifications have not changed the substance of the

agreement embodied in SF 189, and because most agencies have completed implementation of SF 189, the need for retraining has been minimal. ISOO has also responded on an ad hoc basis to the questions of agencies and individuals, and has conducted a number of briefings on recent developments regarding SF 189.

II. 7. If there has been no retraining to teach civil servants the impact of the new "clarifying" rules and modifications for SF 189, is any planned? Under what circumstances would additional training be necessary?

ANSWER: Please refer to the answer to question II. 6., above.

II. 8. The ISOO has stated that liability for release of unclassified information is limited to information being processed under section 1.1(c) of Executive Order 12356 for a final decision on classification status. Is an employee liable for release of unclassified but classifiable information if there is no final decision within 30 days on classification status, as required by section 1.1(c)?

ANSWER: To violate the terms of SF 189, the party disclosing the unclassified information must know or reasonably should know that the information is in the process of a classification determination and that it requires interim protection as provided in Section 1.1(c) of Executive Order 12356. While Section 1.1(c) mandates that agencies make a determination within 30 days, agencies may not always meet this deadline. Failure to meet such a deadline should not, in and of itself, jeopardize the national security. Therefore, it would ordinarily be incumbent upon any reasonable and responsible employee, knowledgeable that a classification determination is in

process, to ascertain the outcome of that decision before releasing the information. Appropriate channels are provided to challenge an agency's failure to meet prescribed deadlines.

II. 9. Please describe fully the procedures to implement section 1.6(a) of E.O. 12356, under which employees may challenge the status of information that they believe has been improperly classified in order to conceal illegality or other misconduct.

ANSWER: Several channels are available to employees who believe that information is classified in violation of the provisions of E.O. 12356. They can challenge the classification through agency security channels, including reliance on Section 3.4 of E.O. 12356, "Mandatory Review for Declassification." Within the Department of Defense, employees are required to challenge the classification of information that they believe to be improperly classified. The National Security Council has approved in principle an ISOO proposal that this standard be required for all agencies. Also, employees may pursue a similar challenge through the agency inspector general.

ISOO is required to consider and take action on complaints and suggestions with respect to the administration of E.O. 12356. Further, ISOO is required under Section 5.4(a) of the Order to report any and all violations to the head of the agency or the senior official responsible for the agency information security program so that corrective steps may be taken. Section 5.4(d) requires that agency heads take appropriate and prompt corrective

action whenever violations occur and that they notify ISOO of such violations.

II. 10. How many challenges of allegedly improper classifications have been filed under section 1.6(a) of E.O. 12356? How many classification decisions have been upheld and how many have been reversed? What is the range and average times to make decisions under section 1.6(a)?

ANSWER: Under Section 5.2(b)(6) of Executive Order 12356, any party may file a complaint with ISOO concerning the administration of the information security program. This provision has been interpreted to include complaints that information has been improperly classified. A thorough review of ISOO's records has revealed only one complaint that alleged that information had been classified "in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security." (E.O. 12356, Section 1.6(a).) This particular complaint resulted in ISOO's review of the classification and declassification decisions of three separate agencies involving hundreds of pages of documents. The matter was resolved in approximately two months, and resulted in the declassification and release of one additional item. ISOO concluded that the rest of the requested information that remained classified following the agencies' classification review was properly classified, and that there was no evidence of any violation of Section 1.6(a) of E.O. 12356.

III. FLOW OF INFORMATION TO CONGRESS

1. What is the definition of a recipient who is "authorized" to receive classifiable information? What is the legal basis for the definition? Please fully describe the distinctions between the status of being "cleared" for receipt of classified information and being "authorized" for receipt of classified or classifiable information, as well as the legal basis for that distinction. Who, if anyone, is inherently "authorized" by virtue of his or her position to receive information covered under SF 189?

ANSWER: As noted repeatedly, it should be clearly understood at the outset that "classifiable information" is information that meets the requirements for classification set forth in E.O. 12356 but is unmarked. There is no distinction between the two for purposes of being "authorized for access."

An individual is "authorized" access to classified information if three conditions are met: First, the individual must have a security clearance; second, the individual must have signed SF 189, or an alternative approved nondisclosure agreement; and third, the individual must have a "need-to-know" the information for an official, authorized purpose. Being "authorized" for access is a function of these three requirements, of which being "cleared" for access is only one. Only the President is inherently "authorized" by virtue of his or her position to receive classified information. The legal basis for access to classified information is Executive Order 12356, "National Security Information."

III. 2. Are all Members of Congress or members of their staffs who sign SF 189s or analogous nondisclosure agreements inherently "authorized" to receive information covered by the agreement? If not, why not? Are all executive branch employees who sign SF 189s "authorized" to receive information covered by the nondisclosure agreement?

ANSWER: Access to classified information is a function of three pre-conditions: A determination of a person's trustworthiness--the security clearance; (2) the signing of SF 189 or an approved alternative nondisclosure agreement; and (3) the exercise of the "need-to-know" principle. A security clearance alone does not automatically give any individual the right of access to particular classified information.

Members of Congress, as constitutionally elected officials, are deemed inherently trustworthy for purposes of eligibility for access, i.e., a clearance. Further, ISOO's rule implementing SF 189 does not require that Members of Congress sign SF 189 as a condition of access to classified information. Members of Congress are not exempt, however, from fulfilling the "need-to-know" requirement. While the need of Congress for information from the executive branch is explicitly acknowledged in the Constitution, no member of Congress is inherently authorized to receive all classified information, but only that which is necessary to perform his or her legislative functions, for example, as a member of a committee or subcommittee that oversees classified executive branch programs.

The three basic requirements for access to classified information mentioned in the opening paragraph apply to congressional staffs as well as executive branch employees. ISOO's regulation implementing SF 189 provides that agency heads may use it as a nondisclosure agreement to be signed by non-executive branch personnel, such as congressional staff members. However, agency heads are free to substitute other agreements for this purpose.

III. 3. What is the definition of congressional "need-to-know"? Does information that the employee reasonably believes evidences illegality, mismanagement, abuse of authority, gross waste or a substantial and specific danger to the public health or safety fall within this "need-to-know" category.

ANSWER: As its name implies, "need-to-know" means that a prospective recipient may be given access to specific classified information only if he or she requires that information to conduct official Government business. The responsibility for determining whether an individual's official duties require access to classified information--and whether the individual meets the standards for access--rests upon the holder of the information, who must act in accordance with agency rules on the subject.

As stated above, the "need-to-know" rule governs access to classified information, that is, information concerning the national defense and foreign relations of the United States, the

unauthorized disclosure of which reasonably could be expected to result in damage to the national security. To prevent an excessively broad interpretation of classification standards, Section 1.6 of Executive Order 12356 explicitly provides limitations on classification. One of these is the prohibition against classifying information "in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security." This provision was included in the Order to help prevent the classification of information that would most likely be the concern of whistleblowers. As an added safeguard against the classification of information that does not meet the established criteria, executive branch agencies provide mechanisms for employees to challenge information in their custody that they reasonably believe to be improperly classified. This would include information that the employee believes evidences illegality, mismanagement, abuse of authority, gross waste or a substantial and specific danger to the public health or safety.

III. 4. Who determines whether Members of Congress or any other potential recipient has a "need to know" classifiable information and what written criteria or guidelines are applied to make this determination. (Please identify all individuals in all covered agencies, by office name and individual name and title, who have this responsibility.)

ANSWER: The policy of this Administration is to comply with congressional requests for classified information to the fullest extent consistent with the constitutional and statutory obligations of the executive branch. Please also refer to the answers to questions III. 1. and 3., above.

III. 5. What is the legal basis for making decisions about who is "authorized" and has a "need-to-know" classifiable information?

ANSWER: Please refer to the answer to question III. 1., above.

III. 6. Does an employee incur liability for making disclosures to Congress under 5 USC 7211 or 18 USC 1505, if the relevant individual or agency office determined that the congressional recipient was not authorized to receive the information under SF 189?

ANSWER: Depending upon the specific facts and circumstances of the disclosure, the employee may or may not be liable for violating the terms of SF 189 in such a situation. The question as posed does not provide enough information to reach any kind of conclusion.

IV. THE TERM "CLASSIFIABLE"

1. Don't the definitions of "classified" in E.O. 12356 and the Industrial Security Manual include proper designation of the information's classified status as a necessary element in the definition of that term? What is the specific legal basis for the ISOO's contention that information can have the legal status of being classified without any markings to that effect?

ANSWER: Before information may be classified in the first instance, i.e., original classification, it must meet four tests. First, an original classification authority must take the action; second, the information must be owned by, produced by or for, or be under the control of the United States Government; third, the information must fall within a classification category, as listed in Section 1.3 of E.O. 12356; and fourth, the original classifier must determine that the unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. Markings, while ordinarily necessary to identify information as classified, have no bearing on the need for classification, that is, the information's national security sensitivity. It is for this purpose that the system designates information, "regardless of its physical form or characteristics," for classification, and not records or some other palpable form. For example, oral communications, which obviously cannot be marked, may just as readily include classified information as written communications, which can and ordinarily should be marked if they include classified information.

IV. 2. What are the laws that permit or require interim marking of documents that have not yet received a final decision on classification status? Is anyone prohibited from marking a document with the notation "Classification determination pending. Protect as though classified. (CONFIDENTIAL, SECRET, or TOP SECRET)," as described on page 49 of the Industrial Security Manual? If not, shouldn't all information be marked with either an interim or final classification status when relevant? If there are marking restrictions, what are all the legal options for employees who generate classified data but do not have the authority to mark its interim or final status?

ANSWER: Section 1.1(c) of Executive Order 12356 requires that in cases of reasonable doubt about the need to classify information, it shall be protected as if it were classified until a classification determination is completed. That determination is to be completed within 30 days. Section 2001.1(b) of ISOO Directive No. 1 (32 CFR § 2001.1(b)), which applies to all executive branch agencies, provides that this information shall be marked in a manner consistent with the marking requirements for classified information. The classification markings for this type of information prescribed in the Industrial Security Manual satisfy the requirements of the ISOO Directive. Ordinarily, all classified information or information for which a classification determination is pending should be marked, assuming it is in a physical form susceptible to being marked. However, the absence of markings does not necessarily mean that the information is not classified or awaiting a classification determination. Please refer to the answer to question IV. 1., above.

IV. 3. Under what circumstances can employees with security clearances mark data as classified information that they generate or discover?

ANSWER: Information may be classified in one of two ways, originally or derivatively. There are three circumstances under which employees with security clearances and proper authorization may mark data as classified information. First, authorized original classifiers may make an initial determination that information requires protection against unauthorized disclosure in the interest of national security. This process includes both the determination of the need to protect the information and, ordinarily, the placement of markings to identify the information as classified. Second, executive branch personnel or Government contractor employees with the appropriate security clearance who are required by their work to restate classified source information must ordinarily apply appropriate security markings on their derivative products. As provided in Section 2.1(a) of E.O. 12356, the derivative classification process is the act of incorporating, paraphrasing, restating or generating in new form classified source information. Information may be derivatively classified in two ways: (a) through the use of a classified source document, usually correspondence or publications generated by an original classification authority; or (b) through the use of a classification guide issued by an original classification authority. Third, Section 1.1(c) of E.O. 12356 provides for reasonable doubt situations. If there is reasonable doubt about

the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority within 30 days. ISOO Directive No. 1 requires that this safeguarding include classification markings, as appropriate.

IV. 4. What liability is incurred by employees without security clearances who disclose classifiable information to unauthorized persons? Has this system of accountability been effective? If not, why isn't that group also required to sign SF 189?

ANSWER: Liability depends solely on the facts and circumstances surrounding an unauthorized disclosure, and the statutes and agency rules that may pertain to these disclosures. The question as posed does not provide enough information to reach any kind of conclusion regarding liability. Uncleared personnel are not lawfully entitled to access to classified information. The SF 189 sets out the rights and obligations of persons who are otherwise lawfully cleared for access to classified information. By definition, it does not apply to uncleared personnel.

IV. 5. What liability is incurred by employees who fail to mark information as classified under their interim or final authority?

ANSWER: Liability depends solely on the facts and circumstances surrounding an unauthorized disclosure. The question as posed does not provide enough information to reach any kind of conclusion regarding liability.

IV. 6. Has the ISOO analyzed the comparative problem of leaks of classified versus classifiable information by civil servants with security clearances and, separately, by employees without security clearances? If not, could such an analysis be performed with existing data?

ANSWER: No. No.

IV. 7. Which laws require civil servants to challenge what they believe are improper decisions to classify information?

ANSWER: Currently there is no specific requirement under E.O. 12356 to challenge improper classification decisions. The classification system, however, has been designed not only to protect information that warrants such extraordinary protection, but to prevent the classification of information that does not warrant it. Therefore, the system provides avenues by which the classification of information may be challenged and reviewed, e.g., Section 3.4 of Executive Order 12356, "Mandatory Review for Declassification." Further, agency regulations establish procedures for employees to challenge the classification of information that they believe is improperly classified. Within the Department of Defense, employees are required to challenge the classification of information that they believe to be improperly classified. Section 2-103 of the Department of Defense Information Security Regulation (DOD 5200.1R) states: "If holders of classified information have substantial reason to believe that the information is classified improperly or unnecessarily, they shall communicate that belief to their

security manager or the classifier of the information to bring about any necessary correction." The National Security Council has approved in principle an ISOO proposal that this standard be required for all agencies.

IV. 8. Do those same laws require civil servants to challenge what they believe are improper decisions to deem information "classifiable"? If so, please describe the legal procedure to challenge improper "classifiable" decisions. Please include all relevant legal citations in your response.

ANSWER: Please refer to the answer to question IV. 7., above.

IV. 9. Although contractors do not make original classification decisions, don't they generate data that becomes classified? Shouldn't the justification for the "classifiability" concept, i.e., that the data is in the process of receiving a final classification decision, apply to contractor employees far more frequently than to civil servants with security clearances? Why are contractor employees held to a lesser standard of liability than civil servants?

ANSWER: Only specified officials of certain Government agencies have original classification authority. Cleared Government contractors may only classify derivatively, based upon instructions provided by a Government official. On occasion, however, contractors may generate data that only becomes classified following review and action by an authorized original classifier. Only a very small portion of "classifiable information," as used in SF 189, refers to information that is in the process of a formal classification determination. We have no evidence to suggest that this happens far more frequently with

data generated by contractors rather than civil servants. Contractor employees are not held to a lesser standard of liability for protecting classified information. However, the Government cannot take some administrative sanctions, e.g., removal from employment, against the contractor employee, because of the absence of an employer/employee relationship.

IV. 10. Has ISOO analyzed the comparative problem of leaks of classifiable versus classified information by civil service employees and, separately, by contractor employees. If not, could such an analysis be performed with existing data.

ANSWER: No. No.

V. INDIRECT DISCLOSURES

1. Is there liability under SF 189 for an employee who discloses classified or classifiable information to a co-worker, if the employee should have known that the co-worker might disclose information to a congressional office that is cleared to receive classified information but not authorized to receive it?

ANSWER: Depending upon the specific facts and circumstances of the disclosure, the employee may or may not be liable for violating the terms of SF 189 in such a situation. The question as posed does not provide enough information to reach any kind of conclusion.

VI. EFFECT ON EMPLOYEES

1. Does the administration stand by the quotations attributed to Mr. Garfinkel in an August 12, 1987, United Press International article, as follows: "An agency manager who believes that an employee has released classified or classifiable information can revoke or suspend his security clearance, or fire, suspend, demote or reprimand him. The manager may seek a legal opinion from the Justice Department or agency counsel before taking action but is not required to do so." If the answer is "yes," does it apply to civil servants generally, or only to those who have signed SF 189 or another nondisclosure agreement?

ANSWER: An appropriate agency manager may take an action, including those listed, against an employee who discloses classified information, and classifiable information as limited by its regulatory definition, whether or not the employee has signed SF 189. The severity of the action will be governed by the facts and circumstances of the case, as permitted by civil service laws and agency regulations. Some agencies require that no action may be taken against an employee without the concurrence of agency counsel.

VI. 2. Please provide the names of the 24 employees with security clearances who refused to sign an SF 189, the agencies with which they are/were affiliated, and the dates they refused to sign. Have any employees without security clearances refused to sign an SF 189?

ANSWER: The reference to the 24 employees with security clearances who had refused to sign SF 189 pertains to that number that had been reported by the agencies to ISOO at the time of the hearing on October 15, 1987. At that time the breakdown was as follows: Air Force, 13 employees; Defense Logistics Agency, one employee; General Services Administration (GSA), one employee;

Next 3 Page(s) In Document Denied

VI. 5. How many employees have been put on an ineligible list for promotions due in whole or in part to their failure to sign SF 189?

ANSWER: None.

VII. EMPLOYEE RIGHTS

1. What is the range of due process rights for employees at various agencies who face disciplinary action, revocation of security clearance or denial of security clearance for failing to sign SF 189? Please provide legal citations for the appropriate regulations at each covered agency as well as the procedures available for the employee to challenge these three potential consequences.

ANSWER: The due process rights of employees would be based on internal agency rules implementing Civil Service laws and regulations, i.e., Chapter 75 of Title 5, United States Code, and Chapter 752 of Title 5, Code of Federal Regulations, respectively. ISOO does not maintain the internal personnel rules of each department, agency and office listed in the answer to question II. 1., above.

VII. 1A. Please provide the same information for an employee charged with violating SF 189.

ANSWER: Please refer to the answer to question VII. 1., above.

VII. 2. Will the administration take any different action against an employee who has not signed SF 189 but discloses classifiable information to an unauthorized person, compared to an employee who has signed SF 189 and makes a prohibited disclosure? If so, please explain the differences.

ANSWER: The Government may seek any remedy available to it to deal with an employee who has made an unauthorized disclosure of classified information, regardless of whether or not he or she has signed SF 189. Failure to sign SF 189 by an individual already having access to classified information does not relieve that person of any responsibilities. The nondisclosure agreement simply makes more explicit the obligations on both the Government and the individual, and gives the latter a better understanding of the actions that may be taken against him or her if he or she fails to live up to these obligations. Also, in stating the nature of these responsibilities in the form of a contractual agreement, SF 189 improves the Government's ability to punish violators through enforcement of the contract.

VIII. CONTRACT ISSUES

1. Assuming that SF 189 is a valid contract, how do the numerous unilateral changes made over the past six months affect its legality?

ANSWER: The regulatory changes, and the prospective inclusion of changes on the form itself, do not affect the legality of SF 189. The substance of the agreement has not been altered. These changes simply clarify perceived ambiguities in the language of SF 189. The rights and duties of the employees who have signed SF 189 have not been changed.

IX. CONFLICT OF LAWS

1. Under SF 189, is an employee liable for making disclosures of information otherwise protected by the whistleblower statute (5 USC 2302(b)(8)) when the Executive begins the process of marking the information classified after the whistleblower exposes misconduct? Put another way, is all unmarked information whose disclosure is not prohibited under other congressional statutes protected despite SF 189, if the whistleblowing employee reasonably believes the information evidences illegality or other misconduct covered under 5 USC 2302(b)(8)? Do disclosures of unmarked but classifiable information disqualify an employee from protection under the whistleblower statute?

ANSWER: The "whistleblower statute" specifically does not extend its protections to employees who disclose classified information without authority. As used in SF 189, "classifiable information" usually refers to unmarked classified information. Therefore, if the employee knows or reasonably should know that the unmarked information is nonetheless classified, the provisions of the "whistleblower statute" should not protect that employee from the consequences of an unauthorized disclosure. In those more limited circumstances where "classifiable information" refers to information that is in the process of a formal classification determination, the applicability of "whistleblower statute" protection should be dependent on the particular facts of the case and the knowledge of the employee regarding the pending determination.

IX. 2. Please list the legal duties that Federal employees have to disclose certain information (i.e., Employee Code of Ethics). When there is a conflict between a statutory duty to disclose and SF 189, which prevails?

ANSWER: There should never be a conflict between any statutes that require disclosure and SF 189, because no statute requires the disclosure of classified information to unauthorized recipients.

IX. 3. Under section 552(b)(1) of the Freedom of Information Act, Executive Branch employees cannot withhold improperly classified data merely because it is marked as classified. Are employees who sign SF 189 required to withhold information that they know or reasonably should know is improperly classified? If so, please provide all legal references in support of this contention.

ANSWER: Except for a situation in which an employee exercises declassification authority over specific information, no employee may unilaterally decide that information is improperly classified. The classification system, however, has been designed not only to protect information that warrants such extraordinary protection, but to prevent the classification of information that does not warrant it. Therefore, the system provides avenues by which the classification of information may be challenged and reviewed, e.g., Section 3.4 of Executive Order 12356, "Mandatory Review for Declassification." Further, ISOO Directive No. 1 (32 CFR Part 2001, at § 2001.34) directs agency heads to process declassification reviews in conjunction with the filing of a Freedom of Information Act request. Agency regulations establish procedures for employees to challenge the

classification of information that they believe is improperly classified. Within the Department of Defense, employees are required to challenge the classification of information that they believe to be improperly classified. The National Security Council has approved in principle an ISOO proposal that this standard be required for all agencies.

X. CLASSIFICATION GUIDE

1. For each system, program, plan, or project involving classified information, there is an information security guide. The Index to these guides lists over 3,700 individual guides. The Index is 370 pages and the individual guides total hundreds if not thousands of pages. Is it the position of ISOO that all individuals with security clearances are chargeable with actual or constructive knowledge of all of the information relating to the classification of information contained in these guides?

ANSWER: Access to classified information is based on an individual's clearance and "need-to-know." "Need-to-know" is based exclusively on that classified information to which an individual must have access in order to perform his or her work related duties. Any one individual has a "need-to-know" a limited amount of classified information. No one, therefore, is expected to be knowledgeable about all the information circumscribed by all existing classification guides.

X. 2. To whom is the Index of Security Classification Guides made available?

ANSWER: The DoD reports that "the Index is routinely available to U.S. Government agencies and their contractors."

X. 3. What is the procedure by which users of the Classification Guides may challenge security classifications reflected in the guides?

ANSWER: Please refer to the answer to question IV. 7., above.

X. 4. Who is the final authority on the proper interpretation and application of a Classification Guide?

ANSWER: The individual who issued the guide, his successor in function, or a supervisory official of either who is responsible for the subject matter of the guide.